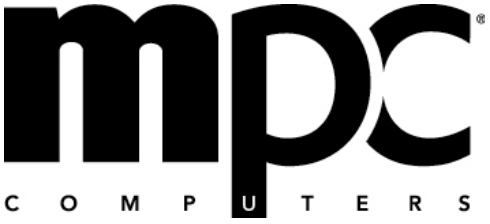


SAN/iQ® Solution Pack for Microsoft® Windows® User Guide

DSM for MPIO VDS Provider
VSS Provider
Authentication Console

This manual is the confidential and proprietary product of LeftHand Networks, Inc. Any unauthorized use, reproduction, or transfer of this manual without the express, written consent of LeftHand Networks, Inc. or its licensee, MPC Computers, LLC is strictly prohibited.

This manual is designed to provide accurate and authoritative information in regard to the use of the DSM for MPIO, the SAN/iQ® VDS Provider, the SAN/iQ® VSS Provider, and the Authentication Console, proprietary products of LeftHand Networks, Inc. Information in this document is subject to change without notice and does not represent a commitment on the part of LeftHand Networks, Inc. or MPC Computers, LLC.

The software described in the document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement.

© Copyright 2006 LeftHand Networks, Inc. All rights reserved. LeftHand Networks, the LeftHand Networks logo, SAN/iQ, and AEBS are registered trademarks of LeftHand Networks, Inc. Distributed Storage Matrix and Remote Copy are trademarks of LeftHand Networks, Inc.

Part # 26200005103 Rev. A

EMA001088-02, MLW, 2/23/2007

Table Of Contents

Chapter 1 DSM for MPIO

Overview 1
Installing SAN/iQ DSM for MPIO 3
Connecting Volumes with the SAN/iQ DSM for MPIO 6

Chapter 2 VDS Provider

Overview 13
Using the VDS Provider 14
Installing the VDS Provider 17
Setting Management Group Credentials 19
Workflow for Using VDS with the iSCSI SAN 20
Working with VDS Volumes 21
Troubleshooting the VDS Provider 23

Chapter 3 VSS Provider

Overview 27
Installing the VSS Provider 27
Setting Management Group Credentials 30
Working with VSS Snapshots 31
Troubleshooting the VSS Provider 32

Chapter 4 Using the Authentication Console

Overview 35
Authenticating Management Groups 35
Entering Management Group Credentials 39
Setting Default Credentials Only 45

Setting Credentials for A New Management Group 45

Index *49*

DSM for MPIO 1

Overview

SAN/iQ® DSM for MPIO enables fault-tolerant paths to the SAN storage modules while also increasing available bandwidth to the SAN for superior performance. When a Windows® Server running iSCSI connects to a volume on the SAN, an active iSCSI session is established to each storage module in the cluster.

SAN/iQ DSM for MPIO enables an application server to continually communicate with the storage module that is hosting a copy of the data that the server is requesting. The SAN/iQ software is able to aggregate the Ethernet connections, processing power and storage capacity of all nodes, increasing performance and capacity as storage modules are added to the network.

Warning: The SAN/iQ DSM for MPIO is the only supported multi-path solution for the MPC DataFRAME® SAN. Using the MS DSM may adversely affect volume and data availability. Therefore, do not install MS MPIO support when installing the MS iSCSI Initiator. If you have installed the MS DSM, we recommend uninstalling it and using the SAN/iQ DSM for MPIO instead.

For more information, including how to uninstall the MS DSM, call MPC Technical Support at 1-800-438-3343.

Device Specific Modules and Microsoft MPIO

The Microsoft MPIO framework allows for storage vendors to write and distribute Device Specific Modules (DSMs) in order to optimally handle multipathing in a SAN environment specific to that vendor. MPIO is a key component to building a Highly

Available, Fault Tolerant SAN solution. MPIO technologies provide for the following:

- I/O Path Redundancy
- I/O Path Failover
- I/O Load Balancing

SAN/iQ DSM for MPIO

Optimized for MPIO in an iSCSI environment based on MPC DataFRAME® iSCSI SAN technologies, the SAN/iQ DSM for MPIO provides for superior path failover and performance capabilities. The MPC DataFRAME® SAN is unique in its distributed system characteristics that give the end-user superior fault tolerance. The SAN/iQ DSM for MPIO further leverages the distributed system technologies and brings those technologies to the Windows iSCSI driver. The SAN/iQ DSM for MPIO provides enhanced MPIO functionality as follows:

- An I/O path is built to each storage module in the cluster on which the volume resides. The SAN/iQ DSM for MPIO handles automatically all the path creation for the Administrator, unlike other native MPIO solutions which require manual path creation.
- Superior performance architecture over native MPIO solutions;
  - Read I/Os are always serviced by a storage module that actually holds a copy of the data being requested.
  - Write I/Os are always serviced by a storage module that holds a copy of the data. Remaining copies (replicas) of the data are forwarded to the appropriate storage module based on the volume replication algorithm (0-way, 2-way or 3-way replication).
- Because an I/O path is built to every storage module in the cluster, a superior fault tolerant solution can be built compared to solutions based on standard MPIO architectures that are typically dual-path only. For instance, if there are 5

storage modules in the cluster, DSM-connected volumes will have 5 iSCSI MPIO connections to the SAN. Four of the five connections could actually go down and I/O would still be serviced.

How the SAN/iQ DSM for MPIO Works

The SAN/iQ DSM for MPIO is a server-side plug-in into the Microsoft iSCSI driver framework. The DSM for MPIO understands the data-map of the volume(s) on the storage cluster according to the iSCSI SAN replication algorithm to read and write to exactly the correct storage node. Figure 1.1 illustrates how the DSM for MPIO driver works with the Microsoft iSCSI driver to build MPIO connections to the SAN.

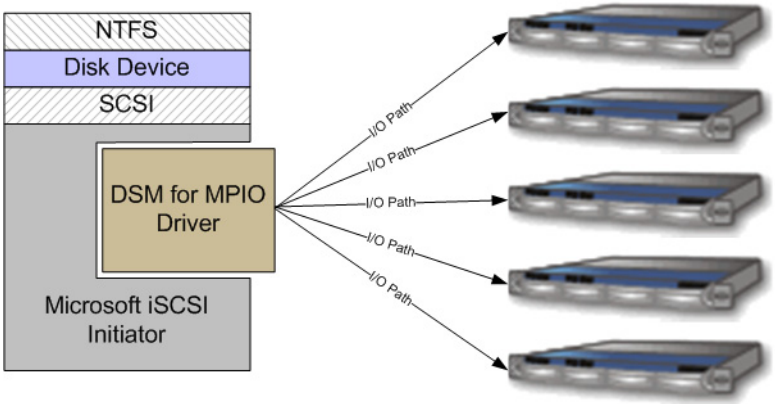


Figure 1.1. Building MPIO connections to the iSCSI SAN

Installing SAN/iQ DSM for MPIO

Prerequisites

- Windows 2003 Server, SP1
- The latest Microsoft iSCSI initiator

- Confirm that Microsoft MPIO Multipathing Support for iSCSI was NOT selected when installing the iSCSI initiator.

  If Microsoft MPIO Multipathing Support for iSCSI is installed, uninstall it before proceeding. For more information, including how to uninstall the MS DSM, call MPC Technical Support at 1-800-438-3343.

If installing DSM for MPIO into an existing Microsoft Cluster,

1. first move all the resources to another cluster node,
2. pause the node on which you plan to install DSM for MPIO.

Upgrading DSM for MPIO

If you are running a previous version of DSM for MPIO

- Uninstall previous version of DSM for MPIO
- Uninstall the MS iSCSI Initiator
- Reboot the server
- Download and install the latest version of the MS iSCSI Initiator. DO NOT select to install the Microsoft MPIO Multipathing Support for iSCSI.

Install SAN/iQ DSM for MPIO

You must reboot the server to complete the installation.

1. Insert the Solution Pack CD in your CD drive.
   The installation wizard opens, shown in Figure 1.2.

Figure 1.2. Installing DSM for MPIO from the Solution Pack CD

2. Click Install.
3. The menu of provider choices opens, shown in Figure 1.3.

Figure 1.3. Choosing the DSM for MPIO to install

4. Click DSM for MPIO.

The installation wizard takes you through the installation process for DSM for MPIO.

Connecting Volumes with the SAN/iQ DSM for MPIO

Once the DSM for MPIO is installed on the server, all iSCSI volume connections made to an iSCSI SAN will attempt to connect via MPIO and the SAN/iQ DSM. There is no need to configure the multiple I/O paths. Simply discover the volumes you wish to connect to and log on.

1. Open the iSCSI Initiator.
2. Enter the VIP address of the cluster on the Discovery tab.
3. Log on to the volumes on the Targets tab, as shown in Figure 1.4.

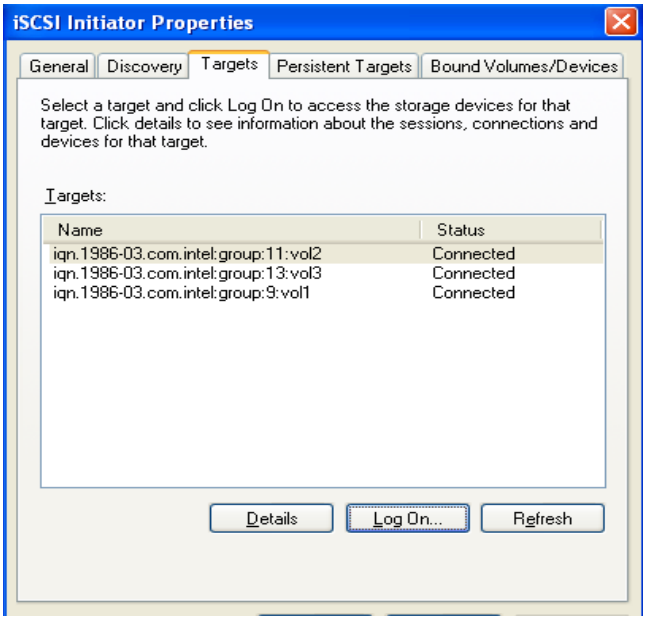


Figure 1.4. Logging on to volumes in the iSCSI Initiator

Verifying DSM for MPIO Operations

After logging on to a volume via iSCSI the DSM for MPIO automatically builds a datapath to each storage module in the cluster. You can verify the DSM for MPIO operations by looking at the Details window of the iSCSI connection for the volume after logging on to the volume, shown in Figure 1.5.

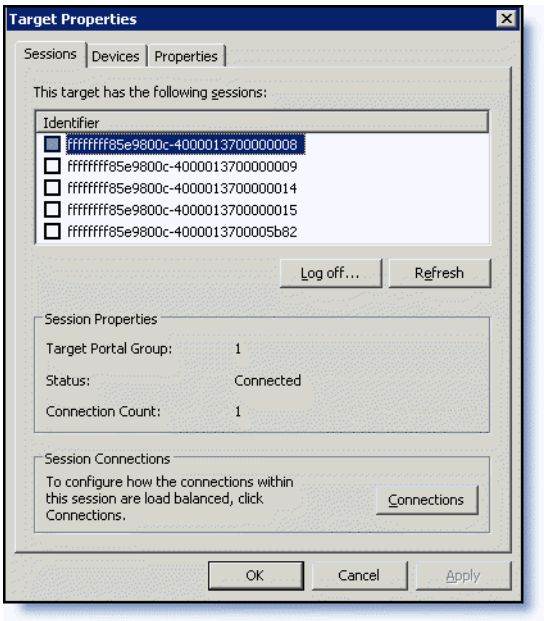


Figure 1.5. Verifying the DSM for MPIO connections to each storage module in the cluster

Configuring DSM for MPIO with Multiple NICs in the Server Connected to the SAN

The SAN/iQ DSM for MPIO supports connecting multiple NICs in the application server to the SAN for fault tolerant physical network connections in the server, as illustrated in Figure 1.6.

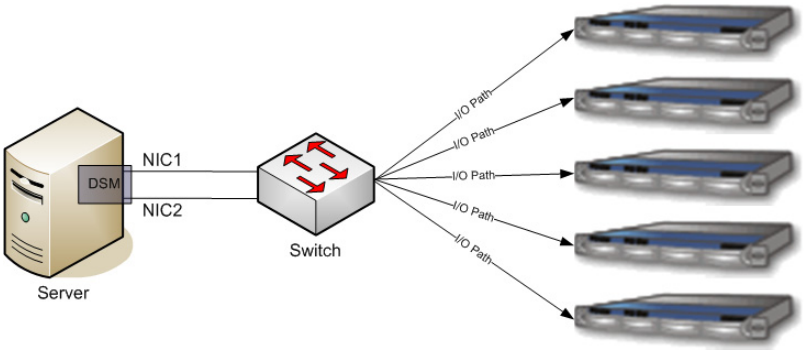


Figure 1.6. Using DSM for MPIO with multiple NICs in the application server

Configure this functionality using the iSCSI Initiator, as follows.

1. Open the iSCSI Initiator and select the volume on the Targets tab.
2. Click Log On.

   The Log On to Target window opens, shown in Figure 1.7.

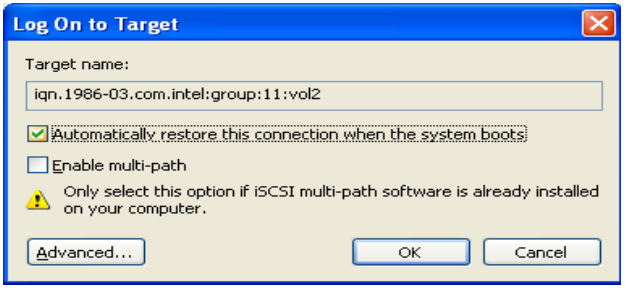


Figure 1.7. Enabling multi-path for DSM

3. [Optional] If you want this volume to be available after rebooting, select the Automatically restore... check box.
4. Select the Enable multi-path check box.
5. Click the Advanced button.

   The Advanced Settings window opens, shown in Figure 1.8.

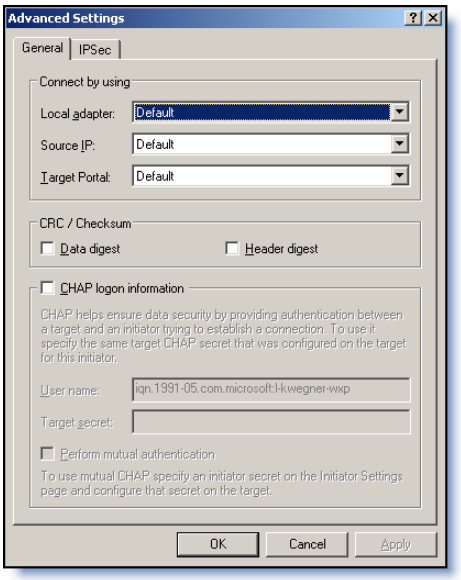

Advanced Settings
General
IPSec
Connect by using
Local adapter:
Default
Source IP:
Default
Target Portal:
Default
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:l-kwegner-wxp
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

Figure 1.8. Configuring iSCSI Initiator advanced settings for DSM for MPIO

6. For Local Adapter, select Microsoft iSCSI Initiator.
7. For source IP, select the IP address of the first NIC you want to use to connect to the volume.
8. For Target Portal, select the VIP of the cluster containing the volume.
9. Click OK to close the Advanced Settings dialog.
10. Click OK to log on to the volume.
11. Repeat these steps for additional NICs.

What Happens if a Path Fails

If an I/O path fails, volume I/O continues since there remains additional active I/O paths to the iSCSI SAN.

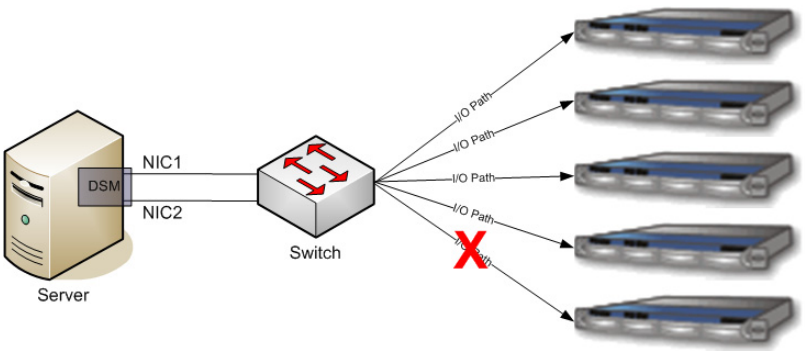


Figure 1.9. Multiple paths ensure continued I/O in event of path failure

When the problem with the I/O path is repaired, the DSM for MPIO re-connects an I/O path to the storage module, thus restoring optimized performance and fault tolerance.

VDS Provider 2

Overview

The VDS Provider supports the Microsoft® Virtual Disk Service (VDS) on the iSCSI SAN. This manual provides general information about using the VDS Provider with your iSCSI SAN. Detailed information about creating and using volumes is available in the iSCSI SAN Online Help or User Manual. You can find detailed information about VDS, DiskRAID and Storage Manager for SANs on the Microsoft web site.

System Requirements

- Windows 2003 Server R2

Glossary

The following terms are used in this chapter.

Table 2.1. Glossary of terms used in this chapter

Term	Definition
Storage Manager for SANs	A storage management tool provided with Windows Server 2003 that runs as a Microsoft Management Console (MMC) plug-in. Use for creating and managing logical unit numbers (LUNs) on the iSCSI SAN.
iSCSI SAN	The Open iSCSI SAN that has the storage volumes.
Console	The management console for the Open iSCSI SAN.
Volume	The iSCSI SAN storage volume.
LUN	The volume created using VDS (DiskRAID and Storage Manager for SANs).
VDS Provider	The hardware provider for using VDS with the iSCSI SAN.

Table 2.1. Glossary of terms used in this chapter

Term	Definition
Windows Virtual Disk Service	The Windows-side VDS tool that works with the VDS Provider.
DiskRAID	The command line tool from Microsoft to create and manage LUNs on the iSCSI SAN.

Using the VDS Provider

The VDS Provider enables you to use MS Windows Server 2003 VDS to create and manage iSCSI SAN volumes and their client server connections. The VDS Provider works with both DiskRAID and Storage Manager for SANs. Figure 2.1 shows the relationship between the VDS Provider, VDS, and the iSCSI SAN.

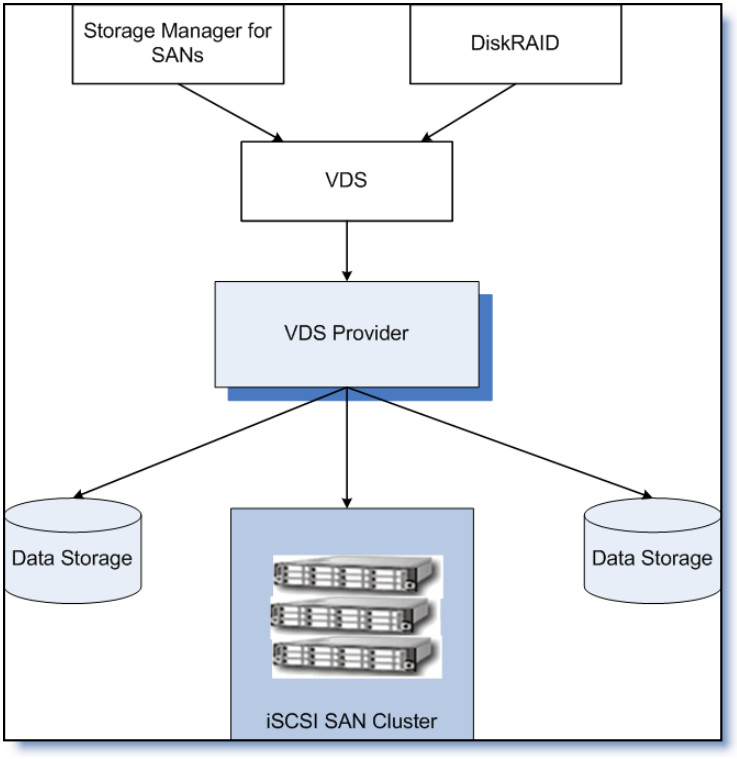


Figure 2.1. Using the VDS Provider with the iSCSI SAN

Using VDS with the iSCSI SAN

While VDS provides volume and client server management tools, some features of the iSCSI SAN are only available from the iSCSI SAN Console. Table 2.2 compares the features of the iSCSI SAN with Storage Manager for SANs.

Table 2.2. Comparing features available in the iSCSI SAN and Storage Manager for SANs

Feature/Function	iSCSI SAN	Storage Manager for SANs
Create LUNs	X	X

Table 2.2. Comparing features available in the iSCSI SAN and Storage Manager for SANs

Feature/Function	iSCSI SAN	Storage Manager for SANs
Assign LUNs to servers	X	X
Configure one-way and mutual CHAP	X	X
Log on to iSCSI targets	-	X
Make iSCSI connections persistent	-	-
Unassign LUNs	X	X
Rename LUNs	-	X
Extend LUNs	X	X
Change volume replication - defaults to 2-way replication or 1-way if only one storage module in cluster	X	-
Configure email alerts	X	-
Change autogrow setting for volumes	X	-
Change volume thresholds	X	-
Create snapshots and snapshot schedules	X	-
Remote copy	X	-

Best Practices for Using the VDS Provider

- Install the VDS Provider on each client server that will connect to the SAN.
- Configure each client locally.

  Refer to the documentation for Storage Manager for SANs for specific information.

Installing the VDS Provider

1. Insert the Solution Pack CD in your CD drive.
   The installation wizard opens, shown in Figure 2.2.

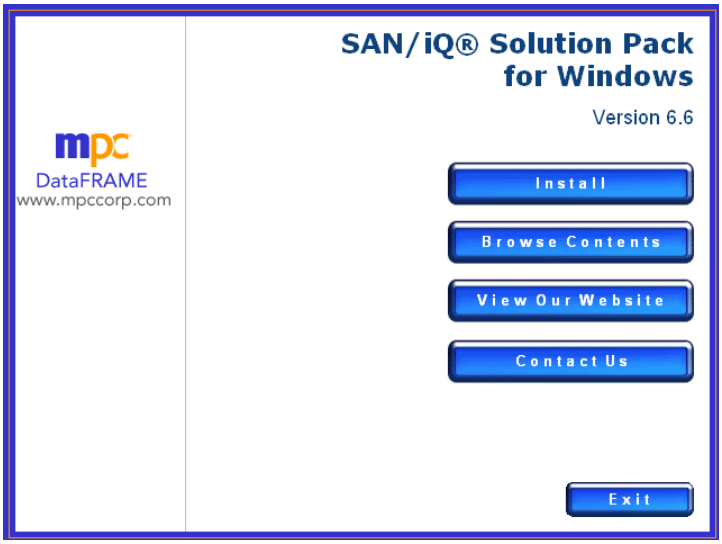


Figure 2.2. Installing the VDS Provider from the Solution Pack CD

2. Click Install.
3. The menu of provider choices opens, shown in Figure 2.3.

Figure 2.3. Choosing the VDS Provider to install

4. Click VDS Provider.

   The installation wizard takes you through the installation process for the VDS Provider.

5. After the VDS Provider is installed, a reminder window opens, shown in Figure 2.4.

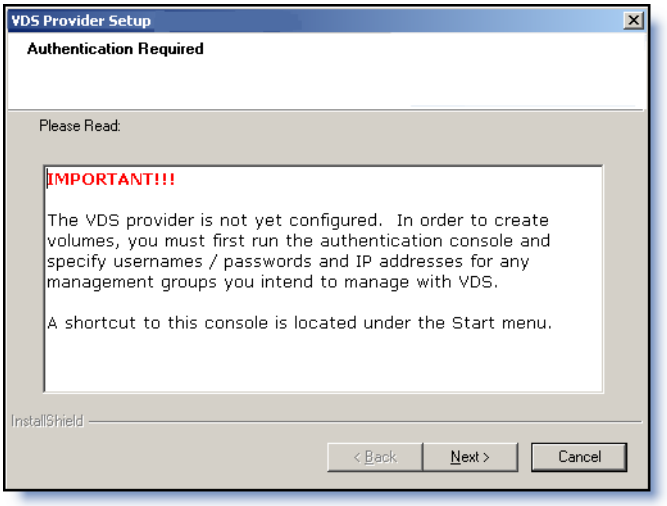

VDS Provider Setup
Authentication Required
Please Read:
IMPORTANT!!!
The VDS provider is not yet configured. In order to create volumes, you must first run the authentication console and specify usernames / passwords and IP addresses for any management groups you intend to manage with VDS.
A shortcut to this console is located under the Start menu.
InstallShield
< Back
Next >
Cancel

Figure 2.4. Authentication reminder

This reminder states that you must open the Authentication Console to configure user names and passwords for management groups

6. Click Next to continue.
7. Click Finish on the final window to complete the wizard.
8. Click Menu on the installer window.

   The Solution Pack installer main window opens.
9. Click Exit to close the installer.

Setting Management Group Credentials

Before using DiskRAID or Storage Manager for SANs, you must set the management group credentials in the Authentication Console. The credentials required for using the VDS provider include:

- management group name
- user name and password
- IP addresses of storage modules that are running managers.

You must also choose to allow VDS control when setting the management group credentials. See Chapter 4, "Using the Authentication Console" for detailed instructions on using the Authentication Console.

Workflow for Using VDS with the iSCSI SAN

While you have some flexibility when using VDS with the iSCSI SAN, some tasks must be done in the Console and in the iSCSI Initiator. Table 2.3 lays out an example workflow for creating volumes with persistent iSCSI connections that you can then connect to clustered servers.

Table 2.3. Example workflow for using VDS with the iSCSI SAN

High-Level Workflow	Specific Tasks
Configure the iSCSI SAN	1. Create the management group and cluster. 2. Make a note of the names of the management group and cluster. 3. Make a note of the IP addresses of the storage modules in the cluster. 4. RECOMMENDED - configure email alerts.
Use the VDS Provider Authentication Console	1. Set the management group credentials
Use DiskRAID or Storage Manager for SANs	1. Create and assign LUNs, including CHAP 2. Logon to iSCSI targets
Use the iSCSI Initiator	1. Make targets persistent
Additional Volume Management Available in the iSCSI SAN	Change autogrow Change volume thresholds Change volume replication Create snapshots Create snapshot schedules Make remote copies of volumes or snapshots
Additional Cluster and Volume Management Available in (DiskRAID or Storage Manager for SANs	Manage MS Clusters Add and remove client servers Enable iSCSI portals Create friendly target names

Best Practices

Configure Email Alerts

Configure email alerts for the storage modules in the iSCSI SAN cluster. Email alerts send notices to all email addresses you configure. With email alerts configured, you do not need to have the Console open to view system alerts for the iSCSI SAN. See the section on *Setting Email Notification* in the Reporting chapter in either the iSCSI SAN User Manual or Online Help.

Make iSCSI Target Persistent

When you log on to the target volume in the iSCSI initiator, select the check box to "Automatically restore this connection when the system boots." Persistent volumes allow the client server to automatically reconnect to the storage volume if a reboot occurs.

Working with VDS Volumes

You can create a VDS LUN on the iSCSI SAN using either DiskRAID or Storage Manager for SANs. The VDS-created volume appears in the Console with the naming convention of "vds-<unique id>" as shown in Figure 2.5.

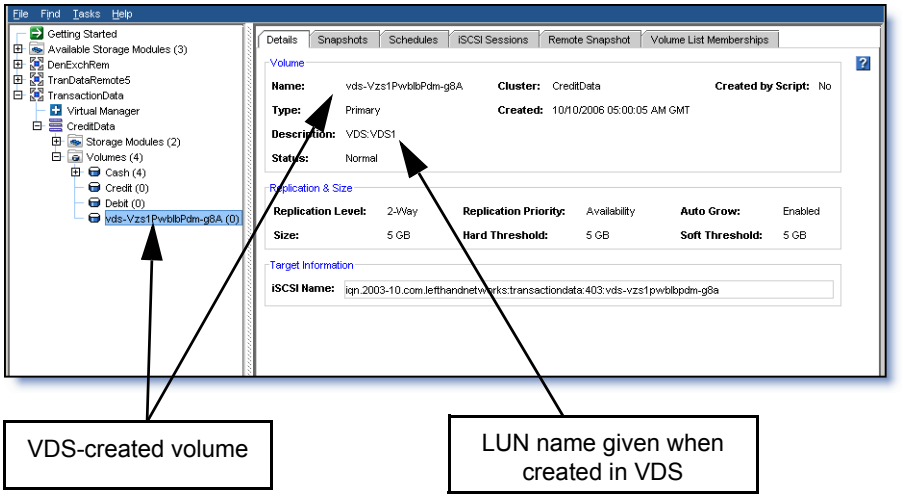


Figure 2.5. Viewing a VDS-created volume in the Console

The volume is created with default characteristics, detailed in Table 2.4t. You can change some of the parameters in the Console using the Edit Volume window. See the SAN User Manual or Console online help for detailed information about the volume parameters.

Table 2.4. Default values for VDS-created volumes

Volume Parameter	Default Value for VDS-Created Volume
Type	Primary
Volume Name	vds-<unique id>
Description	VDS:<LUN name when created in VDS>. Example: VDS:VDS1 **Note:** This field is used by the VDS Provider to display the LUN name you assign when you create the LUN. Do not edit this field in the Centralized Management Console.
Cluster	iSCSI SAN cluster name
Replication Level	◘ 2-way replication if cluster contains 2 or more storage modules. ◘ No replication if cluster contains 1 storage module.
Replication Priority	Availability

Table 2.4. Default values for VDS-created volumes

Volume Parameter	Default Value for VDS-Created Volume
Size	LUN size is set at time of LUN creation. Default value is equal to the available space on the VDS subsystem.
Hard Threshold	Same value as the LUN size
Soft Threshold	Same value as the LUN size
Auto Grow	Disabled

Troubleshooting the VDS Provider

The VDS Provider runs as an NT service. You can view the VDS Provider service in the Computer Management window under Services and Applications > Services, as shown in Figure 2.6.

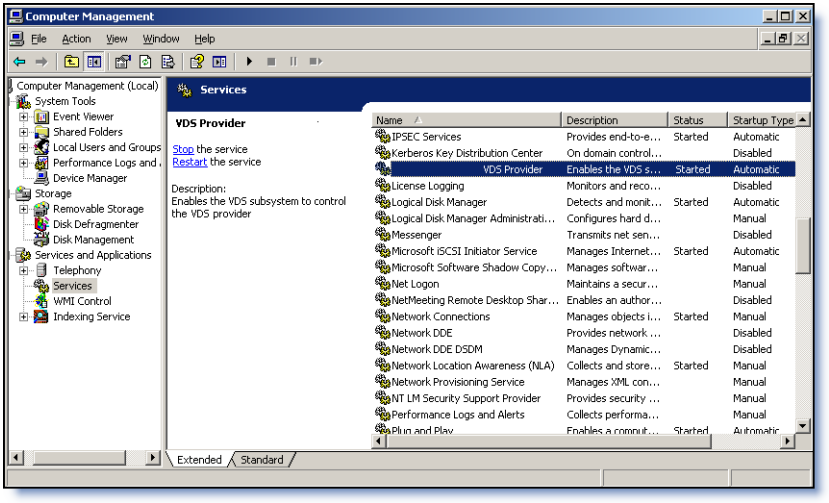


Figure 2.6. Viewing the VDS Provider service

Restarting the VDS Provider Services

The VDS Provider starts automatically. If you check in the Services list and it isn't started, you can start it.

Check the Windows Virtual Disk Service as well. It is listed as Virtual Disk Service. The Virtual Disk Service shuts down after a period of inactivity.

Restarting the Services

Shut down and start up both services as follows.

1. Shut down the VDS Provider service.
2. Shut down the Virtual Disk Service.
3. Start up the Virtual Disk Service.
4. Start up the VDS Provider service.

Viewing the Event Log Messages

The event log reports issues with the VDS Provider and the iSCSI initiator. Open the Application Event Log to view messages about those applications. Check the System Event Log for messages about the Windows Virtual Disk Service.

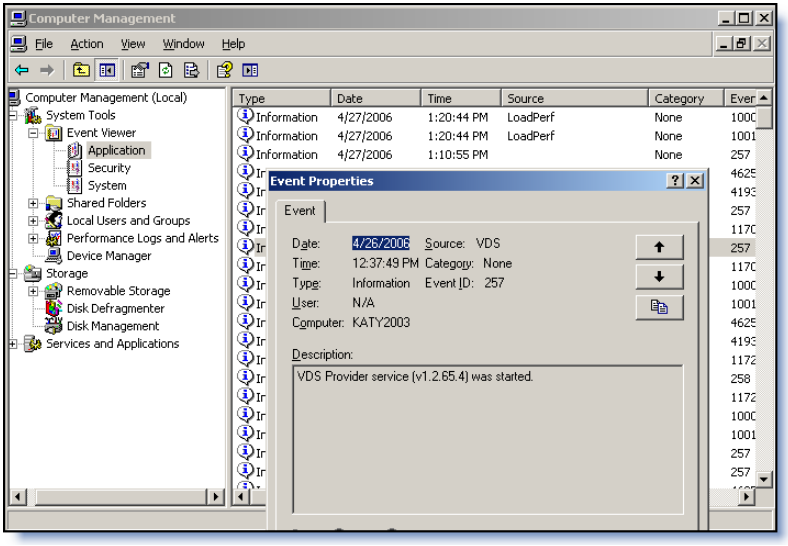


Figure 2.7. Viewing messages in the Event Log

Verify Information in the Authentication Console

Check the information in the Authentication Console. Make sure that the management group has the correct credentials; the user name and password and manager IP addresses.

VSS Provider 3

Overview

The VSS Provider is the hardware provider that supports the Microsoft® Volume Shadow Copy Service (VSS) on the iSCSI SAN. This manual provides general information about using the VSS Provider with your iSCSI SAN. Detailed information about creating and using iSCSI SAN snapshots is available in the iSCSI SAN Online Help or User Manual. You can find detailed information about using the Volume Shadow Copy Service on the Microsoft web site.

System Requirements

- Windows 2003 Server, all versions.

  For transportable snapshots on the Standard version you must install a Microsoft QFE. See "Transportable Snapshots" on page 31 for details.

Installing the VSS Provider

1. Insert the Solution Pack CD in your CD drive.

   The installation wizard opens, shown in Figure 3.1.

Figure 3.1. Installing the VSS Provider from the Solution Pack CD

2. Click Install.
3. The menu of provider choices opens, shown in Figure 3.2.

Figure 3.2. Choosing which provider to install

4. Click VSS Provider.

   The installation wizard takes you through the installation process for the VSS Provider.

5. After the VSS Provider is installed, a reminder window opens, shown in Figure 3.3.

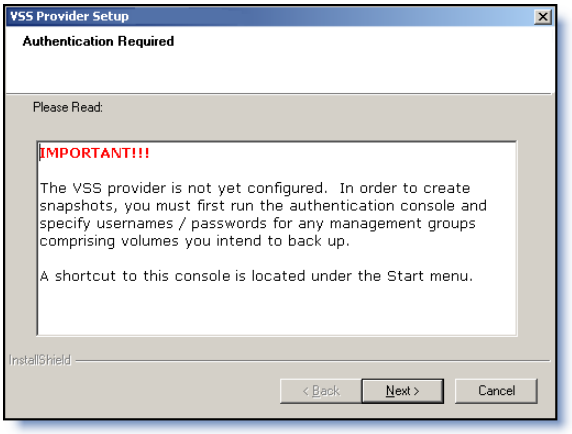

VSS Provider Setup
Authentication Required
Please Read:
IMPORTANT!!!
The VSS provider is not yet configured. In order to create snapshots, you must first run the authentication console and specify usernames / passwords for any management groups comprising volumes you intend to back up.
A shortcut to this console is located under the Start menu.
InstallShield
< Back
Next >
Cancel

Figure 3.3. Authentication reminder

This reminder states that you must open the Authentication Console to configure user names and passwords for management groups

6. Click Next to continue.
7. Click Finish on the final window to complete the wizard.
8. Click Menu on the installer window.

   The Solution Pack installer main window opens.
9. Click Exit to close the installer.

Setting Management Group Credentials

Before using VSS you must set the management group credentials in the Authentication Console. The credentials required for using the VSS provider include:

- management group name
- user name and password

See Chapter 4, “Using the Authentication Console” for detailed instructions on using the Authentication Console.

Working with VSS Snapshots

The VSS Provider creates a VSS snapshot as a persistent target in the MS iSCSI initiator. The VSS snapshot also appears in the Console with the naming convention of "VSS-<unique id>" as shown in Figure 3.4. The snapshot is available as needed to the backup application. Once the snapshot is no longer needed it is deleted from both the Console and the iSCSI initiator.

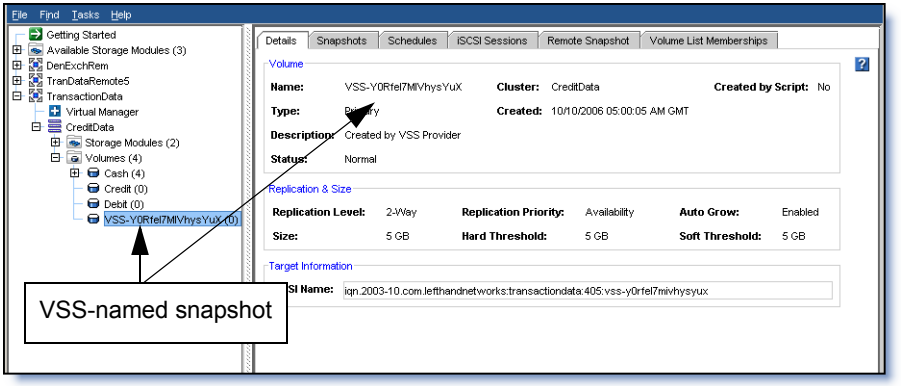
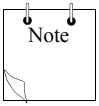


Figure 3.4. Viewing a VSS-named snapshot in the Console

Transportable Snapshots

VSS snapshots can be used as transportable snapshots, that is, they can be mounted on a different server for backup. Transportable snapshots are persistent, which means they will remain in the Console and the iSCSI initiator after the backup completes.



Note: To use transportable snapshots on Windows Server 2003 Standard, you must install the Microsoft QFE referenced in Microsoft Knowledge Base Article: 913648.

Deleting Transportable Snapshots

In order to cleanly delete a transportable snapshot from the system, you should use the requestor application to perform the deletion.

For example, a CommVault QR job requests a transportable snapshot from the VSS Provider. Then, when the snapshot is no longer needed, you can log in to the CommVault application and delete that snapshot which is associated with the job that created it.

Snapshots of Volumes with Auto Grow Disabled

If a volume has auto grow disabled, then VSS snapshots are created with the hard and soft thresholds set to 100% of the volume size.

Snapshots of Volumes with Auto Grow Enabled

When VSS snapshots are created from volumes that have auto grow enabled, then the VSS snapshots are created with a hard threshold of 20% of the volume size and a soft threshold of 15% of the volume size.

For information about how volume size, hard and soft thresholds, and snapshots work, see the chapters about volumes and snapshots in the SAN Online Help or the SAN User Manual.

Troubleshooting the VSS Provider

The VSS Provider runs as an NT service. You can view both the Volume Shadow Copy service and the VSS Provider service in the Computer Management window under Services and Applications > Services.

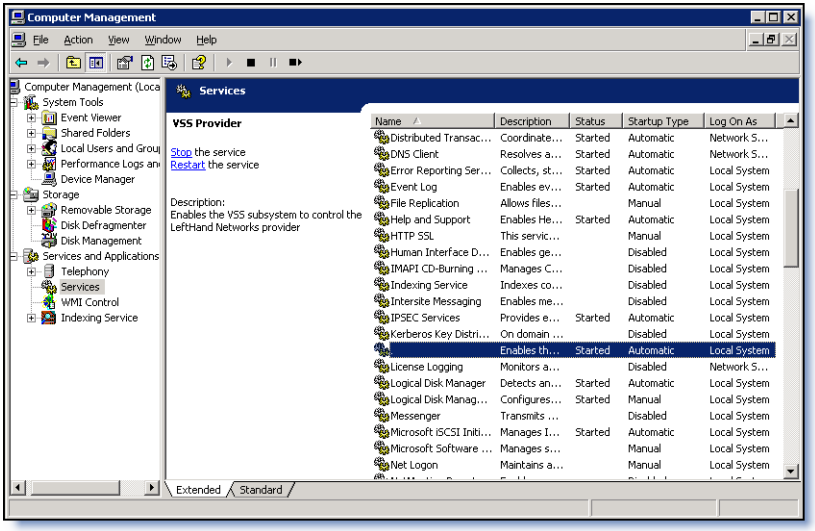

Computer Management
File Action View Window Help
Computer Management (Loca
System Tools
Event Viewer
Shared Folders
Local Users and Grou
Performance Logs an
Device Manager
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
Telephony
Services
WMI Control
Indexing Service
Services
VSS Provider
Stop the service
Restart the service
Description:
Enables the VSS subsystem to control the LeftHand Networks provider
Name
Description
Status
Startup Type
Log On As
Distributed Transac... Coordinate... Started Automatic Network S...
DNS Client Resolves a... Started Automatic Network S...
Error Reporting Ser... Collects, st... Started Automatic Local System
Event Log Enables ev... Started Automatic Local System
File Replication Allows files... Manual Local System
Help and Support Enables He... Started Automatic Local System
HTTP SSL This servic... Manual Local System
Human Interface D... Enables ge... Disabled Local System
IMAPI CD-Burning ... Manages C... Disabled Local System
Indexing Service Indexes co... Disabled Local System
Intersite Messaging Enables me... Disabled Local System
IPSEC Services Provides e... Started Automatic Local System
Kerberos Key Distri... On domain ... Disabled Local System
Enables th... Started Automatic Local System
License Logging Monitors a... Disabled Network S...
Logical Disk Manager Detects an... Started Automatic Local System
Logical Disk Manag... Configures... Started Manual Local System
Messenger Transmits ... Disabled Local System
Microsoft iSCSI Initi... Manages I... Started Automatic Local System
Microsoft Software ... Manages s... Manual Local System
Net Logon Maintains a... Manual Local System
Extended Standard

Figure 3.5. Viewing the VSS Provider service

Restarting the VSS Provider

The VSS Provider starts automatically. If you check in the Services list and it isn't started, you can start it.

Viewing the Event Log Messages

The event log reports issues with the VSS Provider, the iSCSI initiator, and Volume Shadow Copy. Open the Event Log to view messages about those applications.

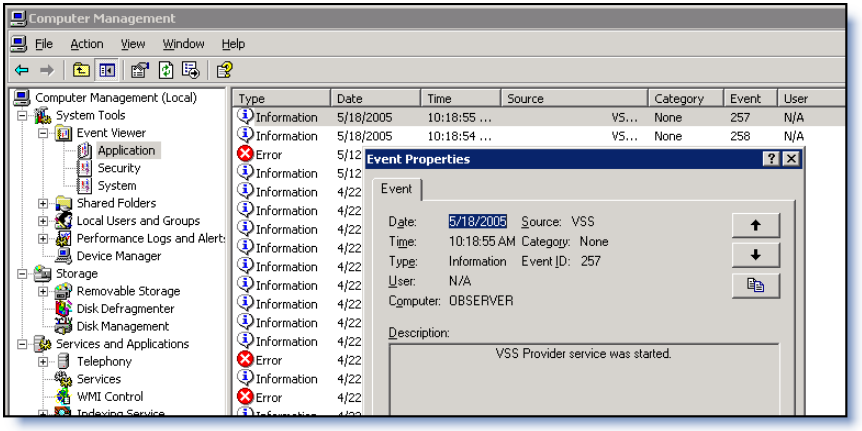


Figure 3.6. Viewing messages in the Event Log

Using the Authentication Console

4

Overview

Use the Authentication Console with both the VSS Provider and the VDS Provider to authenticate management groups on the SAN. Then, when the management groups are authenticated, you can use the Microsoft Volume Shadow Copy Service (VSS) and the Microsoft Virtual Disk Service (VDS) with the SAN.

Authenticating Management Groups

Authenticating management groups on the SAN is the first step for using either the VDS or VSS Provider. You authenticate management groups by setting credentials for them in the Authentication Console. This authentication is normally a one-time process. You would need to redo or update the authentication only if you changed any of the following:

- IP addresses of storage modules
- User name and password for logging in to storage modules
- Which storage modules are in the management group, that is, you added or removed storage modules

Installing the Authentication Console

The Authentication Console is installed automatically when you install either the VSS Provider or the VDS Provider. During the installation for either Provider, a reminder message opens, shown in Figure 4.1, telling you to first run the Authentication Console before creating LUNs or snapshots.

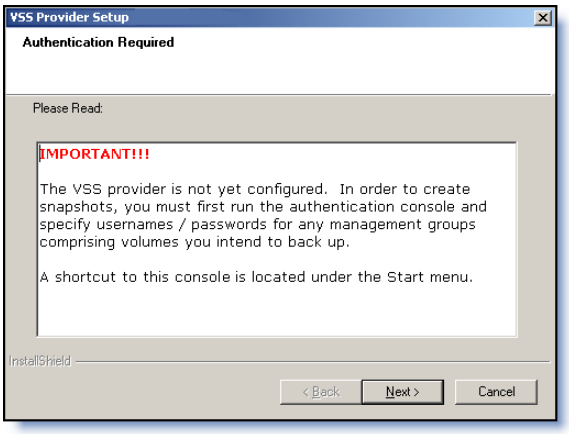

VSS Provider Setup
Authentication Required
Please Read:
IMPORTANT!!!
The VSS provider is not yet configured. In order to create snapshots, you must first run the authentication console and specify usernames / passwords for any management groups comprising volumes you intend to back up.
A shortcut to this console is located under the Start menu.
InstallShield
< Back
Next >
Cancel

Figure 4.1. Reminder to run Authentication Console

Information Needed for Authenticating Management Groups

Prerequisites

You need the following information (credentials) about the management groups you want to authenticate:

VSS and VDS

- Management group name
- User name and password for logging in to the management group. All storage modules in a management group must have the same user name and password.

VDS Only

- IP addresses of storage modules running managers

Choosing Between Default or Individual Credentials

If you use the same user name and password to log into all your storage modules, you can designate default credentials for that user name and password combination.

If you use unique user name and password combinations for storage modules in different clusters or management groups, you can define individual credentials for different management groups.

Setting the Credentials

Credentials for VSS

To use VSS, you must enter the user name and password for storage modules containing the volumes to snapshot.

Credentials for VDS

To use VDS, you must enter the user name and password for storage modules on which you want to create volumes, along with the IP addresses of the storage modules in the management group that are running managers.

Opening the Authentication Console

1. Open the Authentication Console from the Programs menu.

Credentials Wizard

The first time you open the Authentication Console the Credentials Wizard opens, shown in Figure 4.2. At other times, you can open the Credentials Wizard from the Action menu, or the right-click menu. For information about using the Credentials Wizard, see “Setting Default Credentials in the Credentials Wizard” on page 39.

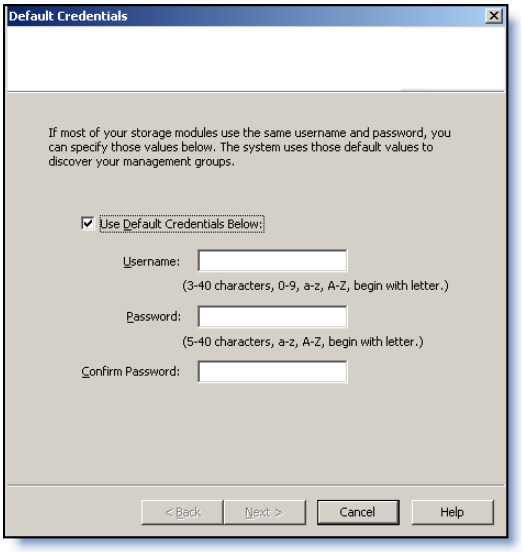

Default Credentials
If most of your storage modules use the same username and password, you can specify those values below. The system uses those default values to discover your management groups.
Use Default Credentials Below:
Username:
(3-40 characters, 0-9, a-z, A-Z, begin with letter.)
Password:
(5-40 characters, a-z, A-Z, begin with letter.)
Confirm Password:
< Back
Next >
Cancel
Help

Figure 4.2. The Credentials Wizard opens the first time you open the Authentication Console

Authentication Console Window

The Authentication Console window, shown in Figure 4.3, opens after you have entered management group credentials.

Discovering Management Groups

The Authentication Console automatically discovers management groups that are on the same subnet as the client you are working on, displayed in the right pane.

If you have a management group on a different subnet, you can add it by adding new management group credentials. See “Setting Credentials for A New Management Group” on page 45.

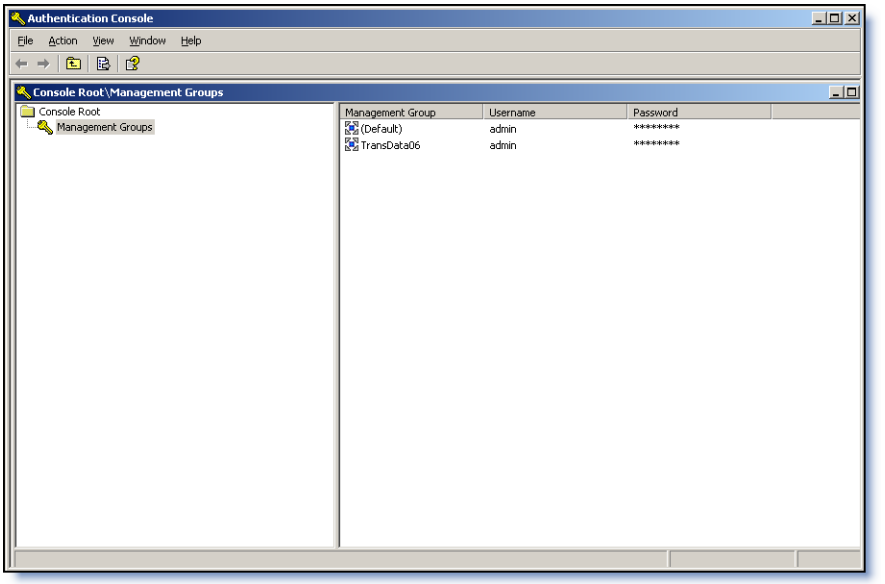


Figure 4.3. Opening the Authentication Console after entering management group credentials

Entering Management Group Credentials

Before using either the VDS or the VSS Provider, you must configure credentials for the management group or groups on the SAN. These credentials include the management group name and the storage module user names and passwords. Also, for VDS, you must enter at least one IP address of a storage module running a manager.

Setting Default Credentials in the Credentials Wizard

In the Credentials Wizard, you can set default credentials for all storage modules that use the same user name and password. The steps required are different for the VSS Provider and the VDS Provider.

The Credentials Wizard opens to the Default Credentials window, shown in Figure 4.4.

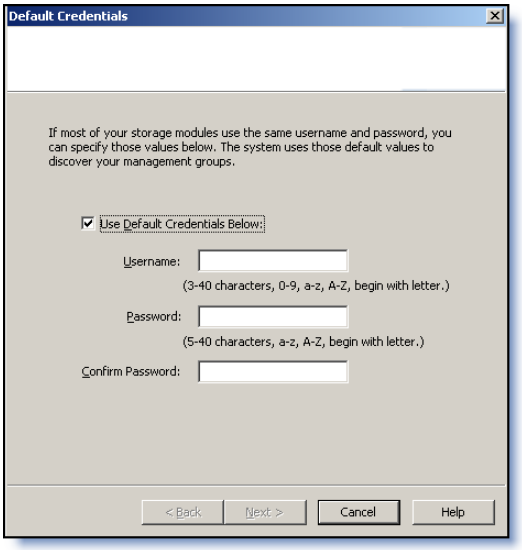

Default Credentials
If most of your storage modules use the same username and password, you can specify those values below. The system uses those default values to discover your management groups.
Use Default Credentials Below:
Username:
(3-40 characters, 0-9, a-z, A-Z, begin with letter.)
Password:
(5-40 characters, a-z, A-Z, begin with letter.)
Confirm Password:
< Back
Next >
Cancel
Help

Figure 4.4. Default Credentials window in the Credentials Wizard

Using VSS Provider

1. On the Default Credentials window, make sure that the Use Default Credentials Below check box is selected.
2. Type in the user name, password, and confirm the password.
3. Click Next.

   The Configure Credentials window opens, shown in Figure 4.5.

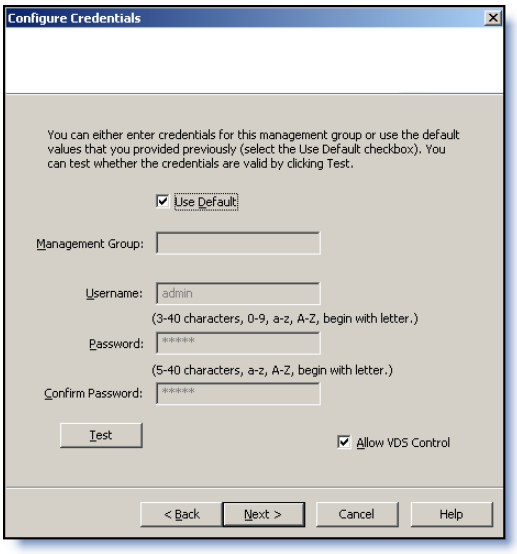

Configure Credentials
You can either enter credentials for this management group or use the default values that you provided previously (select the Use Default checkbox). You can test whether the credentials are valid by clicking Test.
Use Default
Management Group:
Username:
admin
(3-40 characters, 0-9, a-z, A-Z, begin with letter.)
Password:
*****
(5-40 characters, a-z, A-Z, begin with letter.)
Confirm Password:
*****
Test
Allow VDS Control
< Back
Next >
Cancel
Help

Figure 4.5. Configure Credentials window in the Credentials Wizard

4. Clear the Allow VDS Control checkbox and click Next.

   The default credentials are saved and the Authentication Console opens with any management groups it discovered on the subnet listed in the right pane. See Figure 4.6.

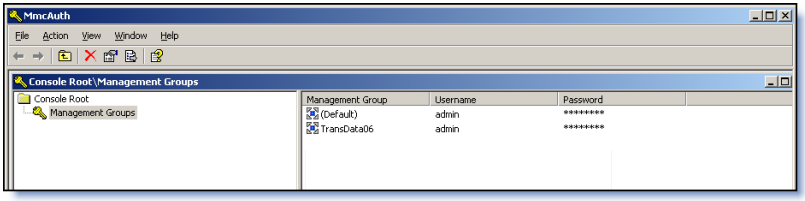


Figure 4.6. Completed management group authentication for VSS

Using VDS Provider

1. On the Default Credentials window, make sure that the Use Default Credentials Below check box is selected.
2. Type in the user name, password, and confirm the password.

3. Click Next.

   The Configure Credentials window opens, shown in Figure 4.5.

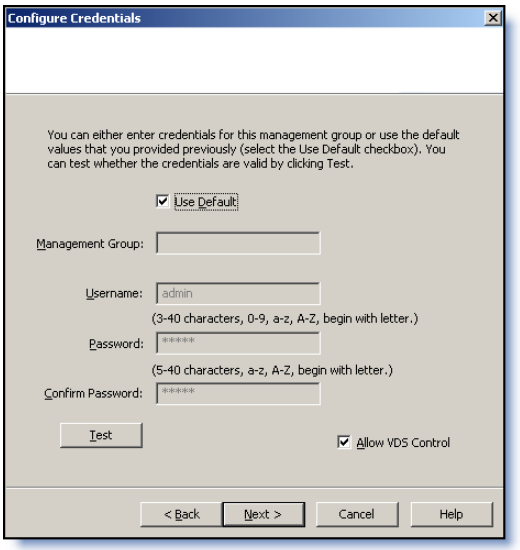

Configure Credentials
You can either enter credentials for this management group or use the default values that you provided previously (select the Use Default checkbox). You can test whether the credentials are valid by clicking Test.
Use Default
Management Group:
Username:
admin
(3-40 characters, 0-9, a-z, A-Z, begin with letter.)
Password:
*****
(5-40 characters, a-z, A-Z, begin with letter.)
Confirm Password:
*****
Test
Allow VDS Control
< Back
Next >
Cancel
Help

Figure 4.7. Configure Credentials window in the Credentials Wizard

4. Make sure the Allow VDS Control checkbox is selected and click Next.

   The window to enter manager IP addresses opens, shown in Figure 4.8.

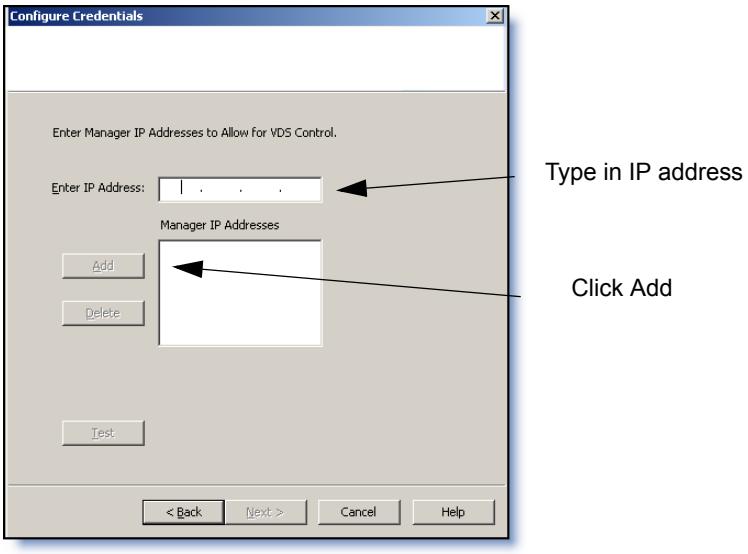


Figure 4.8. Entering manager IP addresses for VDS control

5. Type in the first manager IP address and click Add.
6. Repeat for additional manager IP addresses.
7. Click the Test button to verify the default credentials for the management group listed.

   The test results are reported below the Test button, as shown in Figure 4.9.

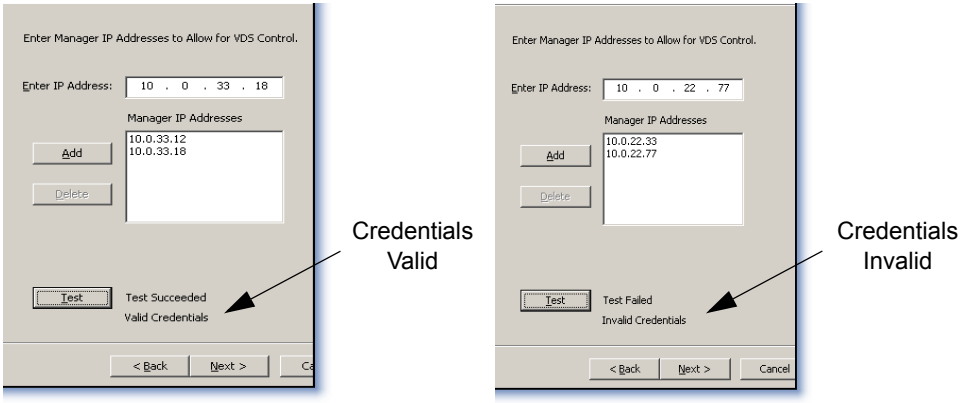


Figure 4.9. Testing the credentials

If the credentials fail as invalid

- Verify the IP addresses you entered
- Verify the user name and password entries

and test them again.

8. When the credentials are verified as valid, click Next.
9. Repeat steps 7 and 8 for additional management groups.
10. Click Finish when you have completed entering IP addresses and validating credentials for all management groups.

    The default credentials are saved and the Authentication Console opens with any management groups it discovered on the subnet listed in the right pane. See Figure 4.10.

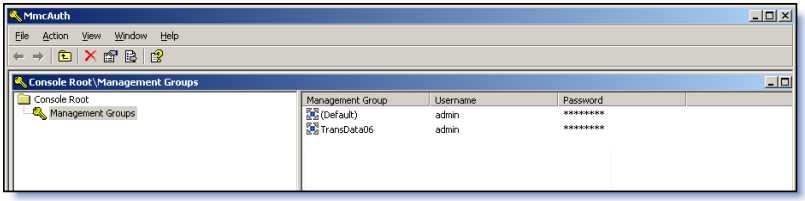


Figure 4.10. Completed management group authentication for VDS

Setting Default Credentials Only

You can, at any time, choose to set default credentials in the Authentication Console without using the Credentials Wizard. Also use this choice to change existing default credentials.

1. From the Action menu, click Set Default Credentials.

   The Default Credentials window opens, shown in Figure 4.11.

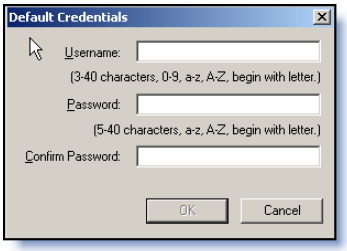


Figure 4.11. Setting default credentials

2. Type in the user name and password and confirm the password.
3. Click OK.

   The default credentials are saved.

Setting Credentials for A New Management Group

Add credentials for a new management group.

1. From the Action menu, click New Management Group Credentials.

   The Management Group Credentials window opens, shown in Figure 4.12.

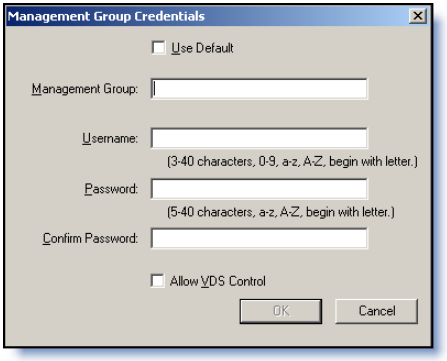


Figure 4.12. Adding credentials for a new management group

1. Type in the management group name and the user name and password.

Using VSS

2. Click OK.

   The Authentication Console window opens with the new management group listed in the right pane.

Using VDS

1. Select the Allow VDS Control checkbox.

   The Management Group Credentials window expands with the Manager IP Address section, as shown in Figure 4.13.

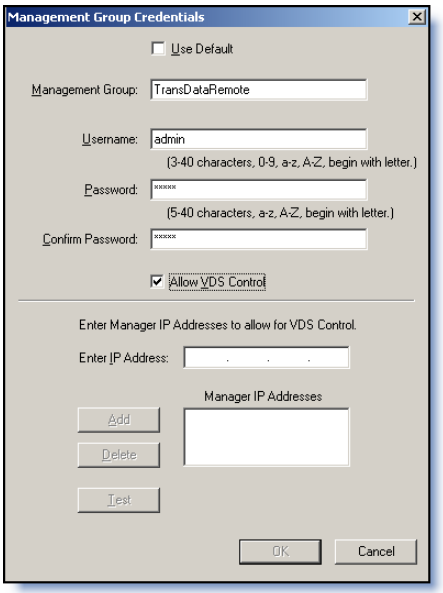


Figure 4.13. New management group credentials with VDS control

2. Type in a manager IP address and click Add.
3. Repeat step 2 to add additional manager IP addresses.
4. Click the Test button to verify the default credentials for the management group listed.

If the credentials fail as invalid

- Verify the IP addresses you entered
- Verify the user name and password entries

and test them again.

5. When the credentials are verified as valid, click OK.

   The Authentication Console window opens with the new management group listed in the right pane.

Deleting a Management Group from the Console

1. Select from the list in the right pane the management group that you want to delete.
2. Right-click and select Delete.

   The management group is deleted from the list.

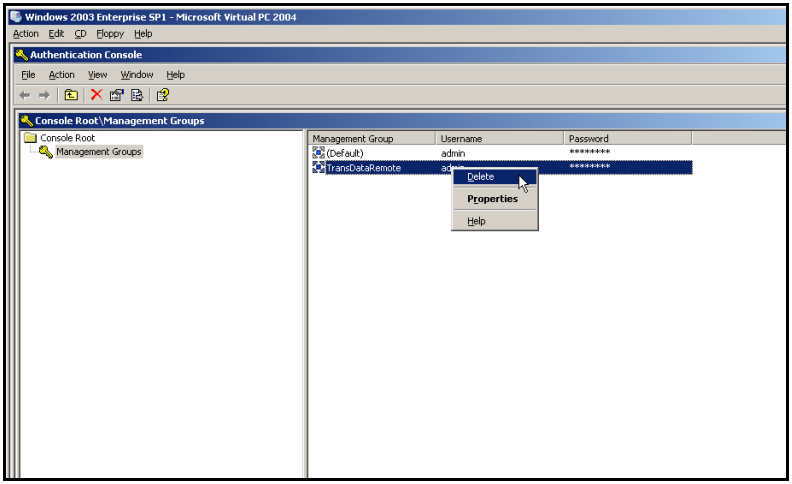
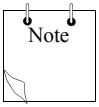


Figure 4.14. Deleting a management group from the Authentication Console



Note: You can also delete default credentials this way.

Index

A

Allow VDS Control Check Box *20*
Authenticating Management Group
  credentials *39*
  for VDS Provider *19*, *36*, *39*, *41*, *46*
  for VSS Provider *30*, *36*, *39*, *46*
  prerequisites for *36*
Authentication Console
  and VDS Provider *19*
  and VSS Provider *30*
  deleting management group *48*
  installing *35*
  opening *37*
Auto Grow
  disabled for volumes, effect of *32*
  enabled for volumes, effect of *32*

B

Best Practice
  configure email alerts on iSCSI SAN *21*
  installing and configuring VDS Provider *16*
  make iSCSI targets persistent *21*

C

Comparing iSCSI SAN and Storage Manager for SANs *15*
Computer Management Window *23*, *32*
Credentials
  for VDS Provider *19*
  for VSS Provider *30*
  management group *39*
  setting for VDS Provider *36*, *39*, *41*, *46*
  setting for VSS Provider *36*, *39*, *46*
Credentials Wizard *39*

D

Default Credentials
  setting for management groups *39*, *45*
Default Values for VDS Volumes *22*
Device Specific Modules *See* DSM
DiskRAID *14*, *19-21*
DSM for MPIO
  and I/O path failure *10*
  configuring for multiple NICs in application server *8*
  connecting volumes with *6*
  installing *4-6*
  overview *1*
  upgrading *4*
  verifying operations *7*
DSM, Microsoft *1*

E
Event Log Messages
VDS Provider *24*
VSS Provider *33*

G
Glossary, VDS Provider
VDS Provider
glossary *13*

I
Installing
Authentication Console *35*
DSM for MPIO *4-6*
VDS Provider *17-19*
VSS Provider *27-30*
iSCSI Initiator *20*, *21*, *24*
iSCSI SAN
best practice, configure email alerts *21*
features compared to Storage Manager for SANs *15*
volume parameters *22*
iSCSI Targets
best practice, make targets persistent *21*

L
Log Messages *See* Event Log Messages

M
Management Group
deleting from Authentication Console *48*
Management Group Credentials
allow VDS control *20*
credentials wizard *39*
setting default credentials *39*, *45*
setting for VDS Provider *20*
Messages, Event Log
VDS Provider *24*
VSS Provider *33*
Microsoft
MPIO *1*
VDS *13*, *35*
VSS *27*, *35*
Microsoft DSM *1*
MPIO, Microsoft *1*

N
NICs
connecting application server using DSM for MPIO *8*

O
Opening Authentication Console *37*
Overview
DSM for MPIO *1*
VDS Provider *13*
VSS Provider *27*

P
Parameters
VDS volumes on iSCSI SAN *22*
Persistent Snapshots *See* Transportable Snapshots
Persistent Targets, iSCSI *21*
Prerequisites for Authenticating Management Groups *36*

S
Server, Application
multiple NICs and DSM for MPIO *8*
Services, NT
VDS Provider *23*
VSS Provider *32*
Setting Management Group Credentials
VDS Provider *19*
VSS Provider *30*
Snapshots, Effect of Auto Grow
when disabled on volumes *32*
when enabled on volumes *32*
Starting
VDS Provider *23*
VSS Provider *33*
Windows Virtual Disk Service *24*
Storage Manager for SANs *13-15*, *19-21*

T
Tasks for Using VDS and iSCSI SAN *20*
Transportable Snapshots *31*
Troubleshooting
VDS Provider *23*
VSS Provider *32*

U
Upgrading DSM for MPIO *4*
User Name and Password *39*
Using VDS *15*, *21*
Using VSS *31*

V
VDS
compared to iSCSI SAN *15*
default values for iSCSI SAN volumes *22*
DiskRAID *14*, *19-21*
Storage Manager for SANs *13-15*, *19-21*
using with iSCSI SAN *15*, *20*, *21*
Windows Virtual Disk Service *24*
VDS Provider
allow VDS control check box *20*
authenticating management groups for *19*
authentication console and *19*
best practice for installing and configuring *16*
credentials for *19*
event log messages *24*
installing *17-19*
overview *13*
running as NT service *23*
setting credentials for *36*, *39*, *41*, *46*
setting management group credentials *19*
starting *23*
troubleshooting *23*
Verifying DSM for MPIO Operations *7*
Virtual Disk Service *See* VDS
Volume Parameters *22*
Volume Shadow Copy Service *See*

VSS
Volumes
connecting with DSM for MPIO *6*
default values for VDS-created iSCSI SAN *22*
VSS *27*
VSS Provider
authenticating management groups for *30*
authentication console and *30*
credentials for *30*
event log messages *33*
installing *27-30*
overview *27*
running as NT service *32*
setting credentials for *36*, *39*, *46*
setting management group credentials *30*
starting *33*
transportable snapshots *31*
troubleshooting *32*

W

Warnings
MS DSM is not supported *1*
Windows Virtual Disk Service, Starting *24*
Wizard, Installation *4-6*, *17-19*
Workflow for Using VDS and iSCSI SAN *20*
Working with VSS Snapshots *31*